UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/564,211	07/25/2006	Johann Arnold	2003P05103WOUS	7536

22116 7590 05/11/2009

SIEMENS CORPORATION
INTELLECTUAL PROPERTY DEPARTMENT
170 WOOD AVENUE SOUTH
ISELIN, NJ 08830

EXAMINER	
ABDALLA, KHALID M	
ART UNIT	**PAPER NUMBER**
2419	

MAIL DATE	DELIVERY MODE
05/11/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/564,211	ARNOLD ET AL.	
	Examiner	Art Unit	
	KHALID ABDALLA	2419	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/24/2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Respond to Amendment

1. This communication is considered fully response to the Amendment filed on 02/24/2009. The following is the new ground rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 8 -14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al (us 2003/0200321A1) in view of Weinstein et al (us 2002/0191572 A1).

Regarding claim 8 Chen discloses an automation network comprising;.

a first subnetwork comprising a first plurality of subscribers (FIG 1 shows plurality of subscribers 'client # 104-110') a second subnetwork comprising a second plurality of subscribers including one or more process devices not configured to provide an end point of a secure tunnel, the second plurality of subscribers(Fig.1 shows another subnet work with plurality of connections 197) including process devices taken from the group consisting of an automation device, a measurement transducer, an operating and monitoring device and a programming device ((FIG 1 shows plurality of subscribers 'client # 104-110' having programming devices 104 and 106);

the network arranged to provide secure data transfer between a first subscriber or multiple ones of the subscribers arranged in the first sub-network and a second

subscriber or multiple ones of the subscribers arranged in the second sub-network (see Fig.1 subnetwork 297 and the plurality of subscribers 'client # 104-110' also see FIG. 2 shows network interface unit 202 logically connected through a tunnel 215 in the Internet to security portal 290 [0052] lines 1-3)

with the first subnetwork comprising at least a first secure-switch connected upstream of the first subscriber or the multiple ones of the subscribers arranged in the first subnetwork, with the second subnetwork comprising at least a second secure-switch connected upstream of at least one process device not capable of producing a tunnel end point (Tunnels in existing systems are typically between firewall nodes that have statically allocated IP addresses. In such existing systems, the statically allocated IP address of the firewall is the address of a tunnel end point within the firewall see [0013] lines 5-9) with the first and second secure switches configured for establishing a secure tunnel having two end points, the first end point being in the first secure switch and the second end point being in the second secure switch(Encryption and encapsulation of data packets for communication with remote nodes or selected other nodes on a LAN to which the subject client machine is connected (collectively, tunnel end points) provides the required secure data transfer see [0025] lines 4-8).

the tunnel configured between the first and second subnetworks to securely transmit data via an insecure network(FIG. 1 shows an overall view of an illustrative LAN (e.g., home-office or telecommuter LAN) 101 as physically connected through the Internet to a corporate headquarters (or main, or other substantial secured network LAN node) internet is insecure network see [0048]lines 1-5) wherein a point-to-point connection is

made between the first subscriber of the first subnetwork and the at least one process device not capable of producing a tunnel end point in the second subnetwork (all data passing through the untrusted net is encrypted by one IPsec-enabled network node and decrypted by another IPsec-enabled node at the other end of the link. In the examples of FIGS. 3 and 4, the illustrative network interface unit of FIG. 4 (302 in FIG. 3) provides IPsec processing, while complementary IPsec processing is performed at security portal 390 in FIG. 3 see [0066] lines 8-14).

Chen does not discloses the secure-switch is an Ethernet switch and at least one port of the tunnel is a layer-3 port for establishing a tunnel end point in accordance with the IPSec-protocol, and wherein, in addition to the secure switch being configured to establish the secure tunnel for at least the first subscriber the connection is made using a subscriber address of the first subscriber,

However Weinstein teaches the secure-switch is an Ethernet switch (FIG. 3A, shows the Ethernet switches 301 and the access points 300 are grouped into two LAN segments see [0051] lines 1-2) and at least one port of the tunnel is a layer-3 port for establishing a tunnel end point in accordance with the IPSec-protocol (all mobile subscriber traffic is encrypted at the IP layer using IPSec see [0089]lines 3-4). And wherein, in addition to the secure switch (The composition of an access point is described with reference to FIG. 3B. Each access point 300 is connected to an Ethernet switch 301-1 to 301-m, where m is the total number of Ethernet switches in the wireless network. As illustrated in FIG. 3A, Ethernet switch 301 is connected to two access points 300 see [0050] lines 5-11),

being configured to establish the secure tunnel for at least the first subscriber the connection is made using a subscriber address of the first subscriber (In order to easily map a mobile terminal address to its corresponding virtual operator, the DHCP server should assign IP addresses on a per virtual operator basis. Note that it is possible that a mobile terminal may belong to multiple VOLANs (multiple virtual operators). In such a case, it may use different interfaces to identify different VOLAN membership with each interface being assigned an IP address see [0082] lines 3-11). Thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to use and modify the arrangement of Chen and couple with both ethernet switch and label switch paths taught by Weinstein in order to provide secure paths for data transmission.

Regarding claim 9, note that Chen discloses the arrangement, further comprising a configuration tool for configuring the automation network (see FIG 1 ,plurality of subscribers 'client # 104-110' configured on the sub network # 101 and see automated configuration and setup [0022]) an, the configuration tool configured to generate parameter data related to the secure-switch and to automatically variety of servers , dedicated processors transmit the generated data to the secure-switch (secure data transfer see [0025].

Regarding claim 10, note that Weinstein teaches the arrangement, wherein the secure-switch (Ethernet switch the core of each PAMLAN see [0057]) comprises at

least one port configured as a WLAN end point (public access mobility LAN and air interface see abstract) for establishing a tunnel end point.

Regarding claim 11, note that Weinstein teaches the arrangement , Wherein the secure-switch comprises at least one port configured to be used as a tunnel end point (subscriber see [0097]), at least one point having a marker (IPsec authentication header generate a codeword over the whole packet [0097]).

Regarding claim 12, note that Weinstein teaches the arrangement, wherein the marker is switchable (IPsec authentication header generate a codeword over the whole packet [0097] also see FIG 8A and FIG 8B)

Regarding claim 13 Chen discloses a secure-switch for securing data access(Encryption and encapsulation of data packets for communication with remote nodes or selected other nodes on a LAN to which the subject client machine is connected (collectively, tunnel end points) provides the required secure data transfer see [0025] lines 4-8) of a first subscriber or a plurality of first subscribers arranged in a first sub-network (FIG 1 shows plurality of subscribers 'client # 104-110') of an automation network to a second subscriber or a plurality of second subscribers arranged in a second sub- network (Fig.1 shows another subnet work with plurality of connections 197)of the automation network, wherein the secure switch is configured to be connected upstream of the first subscriber or the plurality of first subscribers(see

Fig.1 subnetwork 297 and the plurality of subscribers 'client # 104-110' also see FIG. 2 shows network interface unit 202 logically connected through a tunnel 215 in the Internet to security portal 290 [0052] lines 1-3).

Chen does not discloses the secure switch is an Ethernet switch having at least one port embodied as a layer-3- port for establishing a .first tunnel end point in accordance with the IPSec protocol, the secure switch comprising a secure channel converter for establishing a tunnel to a second secure switch connected upstream of the second subscriber or the plurality of second subscribers, the second secure switch being an Ethemet switch having at least one port embodied as a layer-3-port for establishing a second runnel end point in accordance with the IPSec protocol, the first and second tunnel endpoints defining at tunnel configured to securely transmit data via an insecure network, wherein the secure channel converter is configured to establish the tunnel representative for the first subscriber or the plurality of first subscribers and to allocate the tunnel to the first subscriber or the plurality of first subscribers using a subscriber address of the first subscriber or the plurality of first subscribers, thereby effecting, in combination with the second secure switch, a point-to-point connection between at least the first subscriber and the second subscriber.

However Weinstein teaches the secure switch is an Ethernet switch (FIG. 3A, shows the Ethernet switches 301 and the access points 300 are grouped into two LAN segments see [0051] lines 1-2) having at least one port embodied as a layer-3- port for establishing a .first tunnel end point in accordance with the IPSec protocol (all mobile subscriber traffic is encrypted at the IP layer using IPSec see [0089]lines 3-4), the

secure switch comprising a secure channel (Public key based secure channel establishment between the mobile subscriber and the access point see [0088] lines 1-2) converter for establishing a tunnel to a second secure switch connected upstream of the second subscriber or the plurality of second subscribers, the second secure switch being an Ethemet switch (FIG. 3A, shows the Ethernet switches 301 and the access points 300 are grouped into two LAN segments see [0051] lines 1-2) having at least one port embodied as a layer-3-port for establishing a second runnel end point in accordance with the IPSec protocol (all mobile subscriber traffic is encrypted at the IP layer using IPSec see [0089]lines 3-4),, the first and second tunnel endpoints defining at tunnel configured to securely transmit data via an insecure network, wherein the secure channel converter(Public key based secure channel establishment between the mobile subscriber and the access point see [0088] lines 1-2) is configured to establish the tunnel representative for the first subscriber or the plurality of first subscribers and to allocate the tunnel to the first subscriber or the plurality of first subscribers using a subscriber address of the first subscriber or the plurality of first subscribers (In order to easily map a mobile terminal address to its corresponding virtual operator, the DHCP server should assign IP addresses on a per virtual operator basis. Note that it is possible that a mobile terminal may belong to multiple VOLANs (multiple virtual operators). In such a case, it may use different interfaces to identify different VOLAN membership with each interface being assigned an IP address see [0082] lines 3-11), thereby effecting, in combination with the second secure switch, a point-to-point (In FIG. 5, VOLAN 1 has three MPLS paths from access point routers to PAMLAN

gateway routers, and VOLAN 2 has four MPLS paths. LAN segment 1 (602) comprises several air access points. LAN segment 2 (601) is shown with only Ethernet switches ,note that MPLS MPLS neighboring routers usually have point to point connections see [0076]) connection between at least the first subscriber and the second subscriber . Thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to use and modify the arrangement of Chen and couple with secure connection, secure per packet and the public key base channel taught by Weinstein to build up a secure reliable network to transmit data.

Regarding claim14 note that chen discloses the network (see FIG.2) wherein, in addition to the secure switch being configured to establish the secure tunnel (An illustrative network interface unit includes a Dynamic Host Configuration Protocol (DHCP) server, illustratively accessible using a web browser running on a client machine seeking access to VPN nodes. Encryption and encapsulation of data packets for communication with remote nodes or selected other nodes on a LAN to which the subject client machine is connected (collectively, tunnel end points) provides the required secure data transfer see [0025] lines 1-8) for at least the first subscriber, the connection is made using a subscriber address of the first subscriber and an address allocated to the at least one process device not capable of producing a tunnel end point in the second subnetwork, thereby effecting the point-to-point connection (Tunnels in existing systems are typically between firewall nodes that have statically

allocated IP addresses. In such existing systems, the statically allocated IP address of the firewall is the address of a tunnel end point within the firewall see [0013] lines 5-9).

4. Claims 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al (us 2003/0200321A1) in view of Weinstein et al (us 2002/0191572 A1) as applied to claim 13 above and further in view of Aultman et al (US 2005/0021869 A1).

Regarding claim15 chen and Weinstein discloses the secure-switch (Weinstein : FIG. 3A, shows the Ethernet switches 301 and the access points 300 are grouped into two LAN segments see [0051] lines 1-2) .

chen and Weinstein does not discloses the secure-switch further including a secure port, a plurality of non-secure ports, and a switch matrix, with the secure channel converter positioned between the secure port and the switch matrix and with the switch matrix positioned between the secure channel converter and the non-secure ports, so that all data passing through the secure port and into the secure switch pass through the secure channel converter before reaching an unsecured port. However Aultman et al teaches the secure-switch further including a secure port, a plurality of non-secure ports (Each connection to the pairs of port switches 86A, B comprises a secure connection to a first port switch 86A and a non-secure connection to a second port switch 86B see ([0072] lines 19-21 and FIG.8) , and a switch matrix, with the secure channel converter positioned between the secure port and the switch matrix and with the switch matrix positioned between the secure channel (The system 42 provides a control path 46 across the LAN 32 and a data path 48 separate from the LAN 32 The

separate data path 48 provides a communication path between the server(s) 40 and the tape backup library 34 via one or more fiber channels 50 see [0058] lines 9-13) converter and the non-secure ports, so that all data passing through the secure port and into the secure switch pass through the secure channel converter before reaching an unsecured port (a secure backup and recovery network port switch 86A or a non-secure backup and recovery network port switch 86B see [0073] lines 16-18 and FIG.8). Thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to use and modify the arrangement of Chen and Weinstein and couple with the teaching of Aultman et al in order to provide and build up a secure reliable network to transmit and backup data.

Respond to Remarks /Arguments

5. Claim Rejection: Applicant's arguments filed 02/24/2009 have been fully considered but they are not persuasive.

On claim 8, Applicants assert that there is no disclosure in Weinstein " secondary prior art " relating to ethernet switches (e.g. pars 77, 83 and 97) compensates for deficiencies in Chen reference "primary prior art". This argument is not found to be persuasive .The secondary prior art teaches ethernet switches and it does compensate for the deficiencies in Chen reference "primary prior art" (see [0077] lines 6-11 LAN segment 1 (602) comprises several air access points. LAN segment 2 (601) is shown with only Ethernet switches; however, LAN segment 2 (601) could also comprise

several air access points as well. LAN segment 3 (600) is shown with only Ethernet switches; however, LAN segment 3 (600) could also comprise several air access points as well) also see [0083] lines 1-6 "the virtual port contained in each entry of the LIM needs to be augmented with a VLAN tag. This tag identifies the virtual operator in the switched Ethernet LAN the packet will be sent into in order to reach the next neighboring router".

Based on the fact, Examiner respectfully disagrees the prior art recited does not teaches ethernet switches and compensates for deficiencies in the primary reference.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KHALID ABDALLA whose telephone number is (571)270-7526. The examiner can normally be reached on Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dang Ton can be reached on 571-272-3171. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/K. A./
Examiner, Art Unit 2419

/DANG T TON/
Supervisory Patent Examiner, Art Unit 2419/D. T. T./
Supervisory Patent Examiner, Art Unit 2419